



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/715,970	11/17/2003	Sundeep M. Bajikar	42.PI8073	5365

8791 7590 07/26/2007
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER

SHAN, APRIL YING

ART UNIT	PAPER NUMBER
----------	--------------

2135

MAIL DATE	DELIVERY MODE
-----------	---------------

07/26/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/715,970	Applicant(s) BAJIKAR, SUNDEEP M.	
	Examiner April Y. Shan	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 04 May 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>5/2007</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. The Applicant's amendment, filed 04 May 2007, has been received, entered into the record, and respectfully and fully considered.
2. As a result of the amendment, claims 1-4, 9, 13-14 and 18 have been amended. Claims 1-24 are now presented for examination.
3. Any objections/rejections not repeated below for record are withdrawn due to Applicant's amendment.

Information Disclosure Statement

4. The information disclosure statement filed 25 April 2005 fails to comply with 37 CFR 1.98(a)(3) because it does not include a concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR 1.56(c) most knowledgeable about the content of the information, of each patent listed that is not in the English language. It has been placed in the application file, but the information referred to therein has not been considered: DE 10004164A1.
5. The information disclosure statement filed 10 November 2004 contains publications that have not been considered because they are not analogous art or within the same field of endeavor: U.S. Patent No. 5,582,717 (water cooler), U.S. Patent No. 5,720,609 (Catalytic Method for petrol), U.S. Patent No. 5,721,222 (Heterocyclic Ketons – organic biology), U.S. Patent No. 5,796,835 (Sound system enhancement – analog circuit), U.S. Patent No. 6,158,546 (Car muffler).

Claim Objections

6. Claim 9 is objected to because of the following informalities:

a. For claim 9, "exchanging a encryption key" should be "exchanging an encryption key";

Please check the claims 1-24 and correct any informality the Applicant is aware of. Appropriate corrections are required.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 3, 9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per **claims 3 and 9**, "the protected section of memory..." is being recited. However, it lacks of antecedent basis.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under

Art Unit: 2135

the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1-4, 6-16 and 18-24 are rejected under 35 U.S.C. 102(e) as being anticipated by Gehrmann et al. (U.S. Pub. No. 2004/0176071).

As per **claim 1**, Gehrmann et al. discloses a method, comprising:
exchanging data (steps 505 and 506 in fig. 5/steps 605 and 506 in fig. 6)
between a SIM device ("subscription module" – e.g. paragraphs [0065] and [0072]. Please note in paragraph [0017], Gehrmann et al. expressly define the term subscription module comprises modules which may be removably inserted into a communications terminal, such as a SIM card. Therefore, subscription module corresponds to Applicant's SIM device) and an application executed in a trusted platform (e.g. paragraphs [0065]-[0066] and [0084] – [0085]. Please note client communications terminal corresponds to Applicant's an application executed in a trusted platform), via a trusted path within a computer system (e.g. par. [0065] and [0084]), the trusted path being a path through a trusted port ("... The subscription module further comprises an input/output **interface** 206 for communicating with the device it is inserted in..." – e.g. par. [0060], "... the communication over the **interface** provided by the subscription module, is **protected**" – e.g. par. [0022], "... a wireless **interface** and the **subscription module** may be implemented as **one physically inseparable entity**" – e.g. par. [0032], "... Therefore, it is an advantage of the invention that it **secures all interfaces** when providing remote access..." – e.g. par. [0061], [0037] and fig. 2.

Art Unit: 2135

Please note protected interface and secures all interfaces correspond to Applicant's a trusted port) of a chipset (e.g. par . [0036], [0038], [0040], [0049] and [0064]-[0065]. Please note subscription module, processing means, circuit and communication means correspond to Applicant's chipset) wherein the data to be exchanged is secured from unauthorized access ("...thereby providing a considerably improved security against unauthorized use of the sensitive information on the subscription module" – e.g. paragraph [0013], "After successful authentication and key exchange, the actual data exchange between the client communications terminal and the subscription module may be initiated in step 506, preferably using a symmetric encryption algorithm, as described in connection with Fig. 5.." – e.g. paragraph [0085] and "Furthermore, in order to further protect the communication between the RAA client and the subscription module, all messages sent between the entities are integrity protected, as described in connection with Fig. 5...." – e.g. paragraph [0086]).

As per **claim 2**, Gehrmann et al. discloses a method as applied above in claim 1. Gehrmann et al. further discloses wherein the exchanging of data include: exchanging an encryption key via the trusted path within the computer system (e.g. paragraphs [0065] and [0084]); and exchanging data encrypted with the encryption key (e.g. paragraphs [0066] and [0085]), via an untrusted path within the computer system (e.g. paragraph [0022]).

As per **claim 3**, Gehrmann et al. discloses a method as applied above in claim 2. Gehrmann et al. further discloses wherein the exchanging the encryption key includes the application transmitting the encryption key to a protected section of memory within the computer system (e.g. paragraph [0065]); and a SIM device accessing the encryption key from the protected section of memory (e.g. paragraph [0065]).

As per **claim 4**, Gehrmann et al. discloses a method as applied above in claim 2. Gehrmann et al. further discloses wherein the exchanging the encryption key includes the application accessing the encryption key from the SIM device (e.g. paragraph [0065]), the application accessing the encryption key via the trusted port of the chipset (e.g. paragraphs [0064]-[0065]).

As per **claims 6-8 and 12**, Gehrmann et al. discloses a method as applied above in claim 2. Gehrmann et al. further discloses wherein the exchanging data includes a host controller transmitting data from the SIM device to an unprotected section of memory ("The interfaces 304 and 306 may be implemented as plug-in interfaces...such as USB or the like...as the interfaces 304 and/or 306 of the base module are open and, thus vulnerable for unauthorized access..." – e.g. paragraph [0061]. Please note to one with ordinary skill in the art, when using USB, there is a memory section to store USB data packets, which is vulnerable for unauthorized access as disclosed by Gehrmann et al. Therefore, it met the claim limitation of unprotected memory section disclosed by the Applicant),

Art Unit: 2135

wherein the exchanging data includes a driver transmitting data from the unprotected section of memory to the application (e.g. paragraph [0061]), wherein the host controller is a Universal Serial Bus (USB) host controller and the driver is a USB driver (e.g. paragraph [0061]) and further including: exchanging a new encryption key based on a predetermined event selected from a group comprising of, each new transaction, passage of a predetermined period of time (“... the shared secret may be a secret key which is created when needed and which is valid for a specific time period, for one session, or the like, i.e. it is a temporary shared secret” – e.g. paragraphs [0062]) and [0068]-[0071]) and exchange of a predetermined amount of data (e.g. paragraph [0062]).

As per **claim 9**, Gehrmann et al. discloses a method as applied above in claim 2. Gehrmann et al. further discloses wherein the exchanging an encryption key includes the SIM device reading the encryption key from a protected section of memory via the trusted port of the chip set (e.g. paragraph [0064]-[0065]).

As per **claim 10**, Gehrmann et al. discloses a method as applied above in claim 2. Gehrmann et al. further discloses including: the application decrypting the encrypted data using the encryption key (e.g. paragraph [0066]).

As per **claim 11**, Gehrmann et al. discloses a method as applied above in claim 2. Gehrmann et al. further discloses including prior to exchanging the

encryption key, the application authenticating the SIM device (e.g. paragraph [0084] and step 604 in fig. 6).

As per **claim 13**, Gehrman et al. discloses a system comprising: a processor ("a processing unit" – e.g. paragraph [0050]); a memory having a protected section and an unprotected section ("... The key(s) may be stored in the ROM section 203, the EPROM section 204 and/or the RAM section 205, depending on the authentication mechanism and the lifetime of the keys..." – e.g. paragraph [0060] and "...retrieves the public key(s) from its memory, e.g. a ROM or EPROM..." – e.g. paragraph [0079]. Please note ROM section 203, the EPROM section 204 and/or the RAM section 205 for storing keys corresponds to Applicant's protected section of a memory. "The interfaces 304 and 306 may be implemented as plug-in interfaces... such as USB or the like... as the interfaces 304 and/or 306 of the base module are open and, thus vulnerable for unauthorized access..." – e.g. paragraph [0061]. Please note when using USB, there is a memory section to store USB data packets, which is vulnerable for unauthorized access as disclosed by Gehrman et al. Therefore, it met the claim limitation of unprotected memory section disclosed by the Applicant); a SIM device ("...a subscription module 102...the subscription module is a SIM card comprising a processing unit..." – e.g. paragraph [0050]); and a chipset (e.g. par . [0036], [0038], [0040], [0049] and [0064]-[0065]. Please note subscription module, processing means, circuit and communication means correspond to Applicant's chipset) having a trusted port ("... The subscription module further

Art Unit: 2135

comprises an input/output **interface** 206 for communicating with the device it is inserted in...” – e.g. par. [0060], “...the communication over the **interface** provided by the subscription module, is **protected**” – e.g. par. [0022], “...a wireless **interface** and the **subscription module** may be implemented as **one physically inseparable entity**” – e.g. par. [0032], “...Therefore, it is an advantage of the invention that **it secures all interfaces** when providing remote access...” – e.g. par. [0061], [0037] and fig. 2. Please note protected interface and secures all interfaces correspond to Applicant’s a trusted port) to exchange data between the SIM device and an application executed in a trusted platform (e.g. paragraphs [0065]-[0066] and [0084] – [0085]. Please note client communications terminal corresponds to Applicant’s an application executed in a trusted platform), wherein the data to be exchanged is secured from unauthorized access (“...thereby providing a considerably improved security against unauthorized use of the sensitive information on the subscription module” – e.g. paragraph [0013], “After successful authentication and key exchange, the actual data exchange between the client communications terminal and the subscription module may be initiated in step 506, preferably using a symmetric encryption algorithm, as described in connection with Fig. 5...” – e.g. paragraph [0085] and “Furthermore, in order to further protect the communication between the RAA client and the subscription module, all messages sent between the entities are integrity protected, as described in connection with Fig. 5...” – e.g. paragraph [0086]).

As per **claim 14**, Gehrman et al. discloses a system as applied above in claim 13. Gehrman et al. further discloses wherein the exchange of data is to include an exchange of an encryption key via a trusted path within a computer system (e.g. paragraphs [0064]-[0065] and [0084]), and an exchange of data encrypted with the encryption key (e.g. paragraphs [0064]-[0065] and [0085]), via an untrusted path within the computer system (e.g. paragraph [0022]).

As per **claim 15**, Gehrman et al. discloses a system as applied above in claim 13. Gehrman et al. further discloses wherein the exchange of the encryption key includes the application to transmit the encryption key to the protected section of memory (e.g. paragraphs [0064]-[0065]), and the SIM device to access the encryption key from the protected section of memory (e.g. paragraphs [0064]-[0065]).

As per **claim 16**, Gehrman et al. discloses a system as applied above in claim 14. Gehrman et al. further discloses wherein the exchange of the encryption key includes the application to access the encryption key from the SIM device (e.g. paragraphs [0064]-[0065]), the application to access the encryption key via a trusted port of a chipset (e.g. paragraphs [0064]-[0065]).

As per **claim 18**, Gehrman et al. discloses a system as applied above in claim 13. Gehrman et al. further discloses wherein the system includes a host controller to transmit data from the SIM device to an unprotected section of

Art Unit: 2135

memory ("The interface 304 and 306 may be implemented as plug-in interfaces, e.g. using a standard such as USB or the like" – e.g. paragraph [0061]. The interface corresponds to Applicant's host controller).

As per **claims 19-20 and 23**, Gehrmann et al. discloses a system as applied above in claim 14. Gehrmann et al. further discloses wherein the system further includes a driver to transmit data from the unprotected section of memory to the application (e.g. paragraph [0061]), wherein the host controller is a Universal Serial Bus (USB) host controller and the driver is a USB driver (e.g. paragraph [0061]) and wherein the application is to authenticate the SIM device prior to the exchange of the encryption key (e.g. paragraph [0084] and step 604 in fig. 6).

As per **claim 21**, Gehrmann et al. discloses a system as applied above in claim 14. Gehrmann et al. further discloses wherein the SIM device is to read the encryption key from the protected section of memory via a trusted port of the chip set (e.g. paragraphs [0064]-[0065]).

As per **claim 22**, Gehrmann et al. discloses a system as applied above in claim 14. Gehrmann et al. further discloses wherein the application is to decrypt the encrypted data using the encryption key (e.g. paragraph [0066]).

As per **claim 24**, Gehrmann et al. discloses a system as applied above in

claim 14. Gehrman et al. further discloses wherein a new encryption key is to be exchanged based on a predetermined event selected from a group comprising of, each new transaction, passage of a predetermined period of time, and exchange of a predetermined amount of data (e.g. paragraph [0062]).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

13. Claims 5 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gehrman et al. (U.S. Pub. No. 2004/0176071).

As per **claims 5 and 17**, Gehrman et al. discloses a method/system as applied above in claims 2 and 14. Gehrman et al. further discloses wherein the exchanging the encryption key includes exchanging multiple encryption keys (“..multiple keys....” – e.g. paragraph [0060], “a number of secret key codes K-1

Art Unit: 2135

through K-N...the keys may be 128 bit symmetric keys” – e.g. paragraph [0064]), and the exchanging data includes exchanging separate units of data (“...PIN codes, authorization codes, identifiers, account numbers, all messages...” – e.g. paragraph [0066]. Please note all messages such as PIN codes, account numbers corresponds to Applicant’s separate units of data).

Gehrmann et al. does not disclose expressly each unit of data separately encrypted with an encryption key selected from the multiple encryption keys. However, Gehrmann et al. discloses in the paragraph [0062], “the shared secret may be a secret key which is created when needed and which is valid for a specific time period, for one session, or the like, i.e. it is a temporary shared secret”. Therefore, multiple encryption keys can be multiple encryption session keys for encrypting multiple sessions/units of data.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to encrypt each unit of data separately with an encryption key selected from the multiple encryption keys.

The motivation for doing so would have been for the RAA client and the subscription module “to have a shared secret in order to authenticate each other and to protect the communication...for a specific time period”, as taught by Gehrmann et al. (Paragraph [0062]).

Double Patenting

14. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude”

Art Unit: 2135

granted by a patent and to prevent possible harassment by multiple assignees.

A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

15. Claims 1, 2 and 13 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 2, 11, 15, 19 and 23 of copending Application No. 10/977,158 (U.S. Publication No. 2006/0075259). Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1, 2 and 13

encompass the same subject matter as claims 1, 2, 11, 15, 19 and 23 in the copending application.

Claim 1 recites a method comprising: exchanging (The term "exchanging" is interpreted as having the same meaning "transmitting..between" in the copending application) data between a SIM device and an application executed in a trusted platform, wherein the data to be exchanged is secured from unauthorized access (Claim 1, 15, 23 of copending application publication).

Claim 2 recites The method of claim 1, wherein the exchanging of data include: exchanging an encryption key via a trusted path within a computer system; and exchanging data encrypted with the encryption key, via an untrusted path within the computer system (Claim 2 of copending application publication).

Claim 13 recites A system comprising: a processor; a memory having a protected section and an unprotected section; a SIM device; and a chipset to Exchange data between the SIM device and an application executed in a trusted platform, wherein the data to be exchanged is secured from unauthorized access (Claims 11, 19, 23 of copending application publication).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Response to Arguments

16. Applicant's arguments with respect to claims 1 and 13 have been respectfully and carefully considered but are moot in view of the new ground(s) of rejection above using the same reference. (Please see above § 102 and 103 rejections)

17. Applicant's argument on traversing nonstatutory obviousness type double patenting in view of claims 1, 2, 11, 15, 19 and 23 of copending Application No. 10/977,158 is acknowledged, it is not persuasive at this time.

The newly added limitations "via a trusted path within..trust port of a chipset" and "a chipset having a trusted port" in the current application are obvious to a person with ordinary skill in the art in comparison with the co-pending application. Although the conflicting claims are not identical, they are not patentably distinct from each other and encompass the same subject matter. Please note this is nonstatutory obviousness-type double patenting rejection. Therefore, more elements added are not necessarily overcome the rejection. They have to be nonobvious in order for the examiner to consider withdrawing the rejection.

Therefore, due to the above reasons, the examiner maintains the double patenting rejection.

Conclusion

18. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory

Art Unit: 2135

period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Art Unit: 2135


Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


20 July 2007
AYS


KIM VU
PATENT EXAMINER
TECHNOLOGY CENTER 2100